SECURITY REGULATIONS (PROPOSED RULE)
GENERAL PROVISIONS

REGULATION/PG	SUBJECT	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
Part 142 Subpart A	General Provisions				
142.02 Page 43264	Applicability	Applies to: • Health Plan • Health Care Clearinghouse transmitting or receiving standard transaction • Health Care Provider transmitting electronic transaction			
142.104 Page 43265	Reqts for health plans	If standard transaction is conducted with a health plan, the health plan: • May not refuse to conduct the standard transaction • May not delay the transaction on the grounds it is a standard transaction • Health info received and transmitted must be in standard data elements • If conducting transactions through an agent, must make sure agent complies with above			
142.105 Page 43265	Compliance if using clearinghouse	May meet requirements for accepting and transmitting standard transactions by; • Transmitting and receiving standard data elements; or • Through a clearinghouse, submitting nonstandard data elements for conversion to standard data elements and then receiving standard data elements Contract with clearinghouse to receive nonstandard data is not violation of regulations			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.306 Page 43265	Rules for Standard	Standard must be applied to all individual health information electronically maintained or electronically transferred. Clearinghouse that is part of larger organization must protect individual health information from unauthorized access by the organization.	Each entity that is identified as a health plan, health care clearinghouse, and/or health care provider and who electronically maintains or transmits any health information relating to an individual must comply with the security standard.		
142.308 Page 43266	Security Standard	Each entity must access risks and vulnerabilities to individual health data in its possession and develop, implement, and maintain appropriate security measures. Measures must be documented and kept current and must at a minimum contain: NOTE: THE FOLLOWING REGULATIONS CONTAIN DEFINTIONS NOT IDENTIFIED IN THE “DEFINITIONS” SECTION OF THE SECURITY REGS	Standard is to be stable, yet flexible to take advantage of state-of-the-art technology. How individual security requirements are satisfied and which technology to use would be business decisions each organization would have to make. There is a balance between need to secure data against risk and the economic cost of doing so. Entities must consider both aspects in devising their security solutions.		

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) Page 43266	***Administrative procedures to guard data integrity, confidentiality, and availability***	Documented, formal practices to manage selection and execution of security measures to protect data and to manage the conduct of personnel to protect the data. **Procedures include:**	Part of collaborative security regulation development		
142.308 (a) (1) Page 43266	Certification	Technical evaluation of the accreditation process establishing extent to which a particular computer system or network design and implementation meet a specified set of security requirements. May be performed internally or by external accrediting agency.			
142.308 (a) (2) Page 43266	Chain of trust partner agreement	Contract in which two business partners agree to electronically exchange data and protect its integrity and confidentiality.	Agreements are important so that same level of security will be maintained at all links.		

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (3) Page 43266	Contingency Plan	Routinely updated plan for responding to system emergency including: • Performing backups • Preparing facilities to facilitate continuity of operations • Recovering from a disaster **Plan must include ALL of the following:**			
142.308 (a) (3) (i) Page 43266	Applications and data criticality analysis	Entity's formal assessment of sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits.			
142.308 (a) (3) (ii) Page 43266	Data backup plan	Documented, routinely updated plan to create and maintain (for specified period) retrievable, exact, copies of information.			
142.308 (a) (3) (iii) Page 43266	Disaster recovery plan	Part of overall contingency plan that contains a process enabling restoration of any loss of data in event of fire, vandalism, natural disaster, or system failure.			
142.308 (a) (3) (iv) Page 43266	Emergency mode operation plan	Part of overall contingency plan that contains a process enabling continued operation in the event of fire, vandalism, natural disaster, or system failure.			
142.308 (a) (3) (v) Page 43266	Testing and revision procedures	Documented process of periodic testing of written contingency plans to discover weaknesses and the revision of plans if necessary.			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (4) Page 43266	Formal mechanism for processing records	Documented policies and procedures for routine and nonroutine receipt, manipulation, storage, dissemination, transmission and/or disposal of health information.	Important to limit inadvertent loss or disclosure of secure information because of process issues.		
142.308 (a) (5) Page 43266	Information access control	Formal, documented policies and procedures for granting different levels of access to health care information. **Includes all of the following:**			
142.308 (a) (5) (i) Page 43266	Access authorization	Information-use policies and procedures establishing rules for granting access (eg. to a terminal, transaction, program, process or some other user).			
142.308 (a) (5) (ii) Page 43266	Access establishment	Policies and rules that determine entity's initial right of access to a terminal, transaction, program, process or some other user.			
142.308 (a) (5) (iii) Page 43266	Access modification	Policies and rules that determine types of, and reasons for, modification to entity's established right of access to a terminal, transaction, program, process or some other user.			
142.308 (a) (6) Page 43266	Internal audit	In-house review of records of system activity (eg. logins, file accesses, security incidents).	Important to enable organization to identify potential security violations		

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (7) Page 43266	Personnel security	Requires all personnel having access to any sensitive information to have the required authorities as well as all appropriate clearances. **Includes all of the following:**	Important to prevent unnecessary or inadvertent access to secure information		
142.308 (a) (7) (i) Page 43266	Assuring supervision of maintenance personnel by an authorized, knowledgeable person.	Procedures and instructions for oversight of maintenance personnel when personnel are near individual health information.			
142.308 (a) (7) (ii) Page 43266	Maintaining ongoing record of access authorizations	Ongoing documentation and review of levels of access granted.			
142.308 (a) (7) (iii) Page 43266	Assuring operating and maintenance personnel have access authorization	Policies and procedures for determining access level to be granted to individuals working on or near health information.			
142.308 (a) (7) (iv) Page 43266	Establishing personnel clearance procedures	Protective measure to determine that individual's access to sensitive unclassified automated information is admissible.			
142.308 (a) (7) (v) Page 43266	Establishing and maintaining personnel security policies and procedures	Procedures to ensure all personnel who have access to sensitive information have required authority as well as appropriate clearances.			
142.308 (a) (7) (vi) Page 43266	Assuring system users, including maintenance personnel, receive security awareness training.				

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (8) Page 43266	Security configuration management	Coordinated and integrated measures, practices and procedures for the security of information systems. **Includes all of the following:**	Important to ensure that routine changes to system hardware and/or software do not contribute or to create security weaknesses.		
142.308 (a) (8) (i) Page 43266	Documentation	Written security plans, rules, procedures and instructions for all components of entity's security .			
142.308 (a) (8) (ii) Page 43266	Hardware and software installation and maintenance review and testing for security features	Procedures for connecting and loading new equipment and programs, periodic review of maintenance, and periodic security testing of the security attributes of hardware/software.			
142.308 (a) (8) (iii) Page 43266	Inventory	Identification of hardware and software assets.			
142.308 (a) (8) (iv) Page 43266	Security testing	Process used to determine that security features of system are implemented as designed and are adequate for a proposed applications environment. Includes: • Hands-on functional testing • Penetration testing • Verification			
142.308 (a) (8) (v) (A)(B)(C) Page 43266	Virus checking	Act of running computer program that identifies and disables: • Virus computer program that attaches itself to other programs and has the ability to replicate • Code fragment (not an independent program) that reproduces by attaching to another program. • Code embedded in a program that causes copy of itself to be inserted in one or more other programs			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (9) Page 43266	Security incident procedures	Instructions for reporting security breaches. **Includes all of the following:**			
142.308 (a) (9) (i) Page 43266	Report procedures	Mechanism employed to document security incidents			
142.308 (a) (9) (ii) Page 43267	Response procedures	Rules or instructions for actions to be taken as result of receipt of security incident report			
142.308 (a) (10) Page 43267	Security management process	Creation, administration, and oversight of policies ensuring prevention, detection, containment, and correction of security breaches. Involves risk analysis and management Includes: • Establishment of accountability • Management controls (policy and education) • Electronic controls • Physical security • Penalties for abuse and misuse of assets (both physical and electronic **Above includes:**			
142.308 (a) (10) (i) Page 43267	Risk analysis	Cost-effective security/control measures selected by balancing costs of various measures against losses expected if measures were not in place.			
142.308 (a) (10) (ii) Page 43267	Risk management	Assessing risk, taking steps to reduce risk to acceptable level, and maintenance of that level			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (10) (iii) Page 43267	Sanction policies and procedures	Statements regarding disciplinary actions communicated to all employees, agents and contractors. Examples: • Verbal warning • Notice of disciplinary action placed in personnel files • Removal of system privileges • Termination of employment • Contract penalties Must include; • Employee, agent, contractor notice of civil or criminal penalties for misuse or misappropriation of health information • Employee, agent contract notice that violations may result in notification to law enforcement, and regulatory, accreditation and licensure organizations			
142.308 (a) (10) (iv) Page 43267	Security policy	Information values, protection responsibilities, organization commitment for a system. Framework in which entity establishes needed levels of information security to achieve desired confidentiality goals.			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (11) Page 43267	Termination procedures	Instructions, including appropriate security measures for ending of employment or internal/external user's access **Includes all of the following:**			
142.308 (a) (11) (i) Page 43267	Changing locks	Changing combinations of locking mechanisms: • On a recurring basis • When personnel no longer have need to know or require access to protected facility or system			
142.308 (a) (11) (ii) Page 43267	Removal from access lists	Physical eradication of entity's access privileges			
142.308 (a) (11) (iii) Page 43267	Removal of user accounts	Termination or deletion of individual's access privileges to information, services, and resources when clearance, authorization and need-to-know no longer exists.			
142.308 (a) (11) (iv) Page 43267	Turning in of keys, tokens or cards allowing access	Procedure to ensure all physical items allowing a terminated employee to access property, building, or equipment are retrieved from employee, preferably before termination			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Administrative procedures to guard data integrity, confidentiality, and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (a) (12) Page 43267	Training	Education concerning vulnerabilities of health information and ways to ensure protection of that information **Includes all of the following:**			
142.308 (a) (12) (i) Page 43267	Awareness training for all personnel, including management	Training in security awareness that includes: • Password maintenance • Incident reporting • Viruses and other forms of malicious software			
142.308 (a) (12) (ii) Page 43267	Periodic security reminders	Employees, agents, contractors made aware of security concerns on ongoing basis			
142.308 (a) (12) (iii) Page 43267	User education concerning virus protection	Training relative to user awareness: • Potential harm caused by virus • How to prevent introduction of virus • What to do if virus detected			
142.308 (a) (12) (iv) Page 43267	User education in monitoring log-in success or failure and how to report discrepancies	Training in user's responsibility to ensure security of health care information			
142.308 (a) (12) (v) Page 43267	User education in password management	Training in rules creating and changing passwords and need for confidentiality			

SECURITY REGULATIONS (PROPOSED RULE)
SECURITY STANDARD (CONTINUED)
Physical safeguards to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (b) Page 43267	***Physical safeguards to guard data integrity, confidentiality and availability***	Protection of computer systems and related buildings and equipment from fire and other natural and environmental hazards as well as from intrusion. Covers use of locks, keys and administrative measures to control access **Includes all of the following:**			
142.308 (b) (1) Page 43267	Assigned security responsibility	Practices established by management to manage and supervise execution and use of security measures to protect data and manage and supervise conduct of personnel in the protection of data			
142.308 (b) (2) Page 43267	Media controls	Policies and procedures governing receipt and removal of hardware/software (e.g. diskettes and tapes) **Includes all of the following:**			
142.308 (b) (2) (i) Page 43267	Access control				
142.308 (b) (2) (ii) Page 43267	Accountability	Property ensuring actions of entity can be traced uniquely to entity			
142.308 (b) (2) (iii) Page 43267	Data backup	Retrievable, exact copy of information			
142.308 (b) (2) (iv) Page 43267	Data storage	Retention of individual health information in an electronic format			
142.308 (b) (2) (v) Page 43267	Disposal	Final disposition of electronic data and/or hardware on which data is stored			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Physical safeguards to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (b) (3) Page 43267	Physical access controls	Policies and procedures limiting physical access to entity while ensuring properly authorized access is allowed **Includes all of the following:**			
142.308 (b) (3) (i) Page 43267	Disaster recovery	Process enabling entity to restore loss of data in event of fire, vandalism, natural disaster, or system failure			
142.308 (b) (3) (ii) Page 43267	Emergency mode operation	Access controls enabling entity to continue operation in event of fire, vandalism, natural disaster, or system failure			
142.308 (b) (3) (iii) Page 43267	Equipment control (in and out of site)	Procedures for bringing hardware and software into and out of building and maintaining record of that equipment Includes (for hardware and storage media: • Marking • Handling • Disposal			
142.308 (b) (3) (iv) Page 43267	Facility security plan	To safeguard premises and building (exterior and interior) and equipment from unauthorized physical access, tampering, theft			
142.308 (b) (3) (v) Page 43267	Verifying access authorizations before granting physical access	Policies and instructions for validating access privileges of entity			
142.308 (b) (3) (vi) Page 43267	Maintenance records	Documentation of repairs and modifications to physical components of facility			
142.308 (b) (3) (vii) Page 43268	Need-to-know procedures for personnel access	Security principle stating a user should have access only to data he or she need to perform a particular function			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Physical safeguards to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (b) (3) (viii) Page 43268	Procedures to sign-in visitors and provide escorts, if appropriate	Procedure governing reception and hosting of visitors			
142.308 (b) (3) (ix) Page 43268	Testing and revision	Restriction of program testing and revision to formally authorized personnel			
142.308 (b) (4) Page 43268	Policy and guidelines on work station use	Instructions/procedures delineating: • Proper functions to be performed • Manner in which those functions are to be performed • Physical attributes of surrounding of specific computer terminal site or type of site dependent upon sensitivity of information accessed from that site			
142.308 (b) (5) Page 43268	Secure workstation location	Physical safeguards to eliminate or minimize possibility of unauthorized access to information - Example: • Locating terminal used to access sensitive information in locked room and restricting access to authorized personnel • Not placing terminal used to access patient information in any area of doctor's office where screen contents could be viewed from reception area			
142.308 (b) (6) Page 43268	Security awareness training	Training programs in which all employees, agents, contractors must participate, including: • Based on job responsibilities • Customized education programs focusing on issues regarding use of health information • Responsibilities regarding confidentiality and security			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Technical security services to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (c) Page 43268	***Technical security services to guard data integrity, confidentiality and availability***	Processes put in place to protect information and control individual access to information **Includes the following:**			
142.308 (c) (1) Page 43268	Technical security services	**Must include all of the following:**			
142.308 (c) (1)(i) Page 43268	Access control	**Includes:**			
142.308 (c) (1)(i)(A) Page 43268	Procedure for emergency access	Instructions of obtaining necessary information during crisis			
142.308 (c) (1)(i)(B) Page 43268		At least one of the following:			
142.308 (c) (1)(i)(B)(1) Page 43268	Context-based access	Access control procedure based on context of transaction (as opposed to being based on attributes of initiator or target			
142.308 (c) (1)(i)(B)(2) Page 43268	Role-based access				
142.308 (c) (1)(i)(B)(3) Page 43268	User-based access				
142.308 (c) (1)(i)(C) Page 43268	Optional use of encryption				
142.308 (c) (1)(ii) Page 43268	Audit controls	Mechanisms employed to record and examine system activity			
142.308 (c) (1)(iii) Page 43268	Authorization control	Mechanism for obtaining consent for use and disclosure of health information **Includes at least one of following:**			
142.308 (c) (1)(iii) (A) Page 43268	Role-based access				
142.308 (c) (1)(iii) (B) Page 43268	User-based access				

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Technical security services to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (c) (1)(iv) Page 43268	Data authentication	Corroboration that data has not been altered or destroyed in unauthorized manner. Includes use of: • Check sum • Double keying • Message authentication code • Digital signature			
142.308 (c) (1)(v) Page 43268	Entity authentication	Corroboration that entity is one claimed **Includes :**			
142.308 (c) (1)(v)(A) Page 43268	Automatic logoff	Security procedure that causes an electronic session to terminate after predetermined time of inactivity			
142.308 (c) (1)(v)(B) Page 43268	Unique user identifier	Combination name/number assigned and maintained in procedures for identifying and tracking individual user identity			
142.308 (c) (1)(v)(C) Page 43268		**At least one of the following:**			
142.308 (c) (1)(v)(C)(1) Page 43268	Biometric identification	Identification system that identifies a human from a measurement of physical feature or repeatable action of individual Examples: • Hand geometry • Retinal scan • Iris scan • Fingerprint patterns • Facial characteristics • DNA sequence characteristics • Voice prints • Hand written signature			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Technical security services to guard data integrity, confidentiality and availability

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (c) (1)(v)(C)(2) Page 43268	Password				
142.308 (c) (1)(v)(C)(3) Page 43268	Personal identification number (PIN)	Number or code assigned to individual and used to provide verification of identity			
142.308 (c) (1)(v)(C)(4) Page 43268	Telephone callback procedure	Method of authenticating identity of receiver and sender of information through series of questions and answers sent back and forth establishing identity of each Example: • When communicating systems exchange series of identification codes as part of initiation of a session to exchange information • When a host computer disconnects initial session before authentication is complete and host calls user back to establish a session at a predetermined telephone number			
142.308 (c) (1)(v)(C)(5) Page 43268	Token				

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Technical security mechanisms

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (d) Page 43268	***Technical security mechanisms***	Processes to guard against unauthorized access to data transmitted over a communications network			
142.308 (d)(1) Page 43268	If entity uses communications or network controls…	**Entity's technical security mechanisms must include following:**			
142.308 (d)(1)(i) Page 43268		**The following implementation features:**			
142.308 (d)(1)(i)(A) Page 43268	Integrity controls	Security mechanism employed to ensure validity of information being electronically transmitted or stored			
142.308 (d)(1)(i)(B) Page 43268	Message authentication	Ensuring, typically with message authentication code that a message received (usually via a network) matches the message sent			
142.308 (d)(1)(ii) Page 43268		**One of the following:**			
142.308 (d)(1)(ii)(A) Page 43268	Access controls	Protection of sensitive communications transmissions over open or private networks so they cannot be easily intercepted and interpreted by parties other then intended recipient			
142.308 (d)(1)(ii)(B) Page 43268	Encryption				

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Technical security mechanisms

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.308 (d)(2) Page 43268	If entity uses network controls to protect sensitive communication transmitted over open networks so it cannot be easily intercepted and interpreted by parties other then intended recipient	**Entity's technical security mechanisms must include all of the following:**			
142.308 (d)(2)(i) Page 43268	Alarm	Any device that can sense abnormal condition within the system and provide, either locally or remotely, a signal indicating presence of abnormality. Signal may be in any desire form ranging form simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle			
142.308 (d)(2)(ii) Page 43268	Audit trail	Data collected and potentially used to facilitate a security audit			
142.308 (d)(2)(iii) Page 43268	Entity authentication	Communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes			
142.308 (d)(2)(iv) Page 43268	Event reporting	Network message indicating operational irregularities in physical elements of network or response to the occurrence of significant task, typically the completion of request for information.			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Electronic signature standard

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.310 Page 43268 and 43269	***Electronic signature standard***				
142.310 (a) Page 43268 and 43269	If entity elects to use electronic signature in a transaction or such a signature is required by the Secretary	**Entity must apply the following electronic signature standard**			
142.310 (b) Page 43269	Standard				
142.310 (b)(1) Page 43269	Electronic signature	The attribute affixed to electronic document to bind it to a particular entity Secures user authentication (proof of claimed identity) at the time signature is generated Creates logical manifestation of signature (including possibility for multiple parties to sign a document and have the order of application recognized and proven Supplies additional information such as time stamp and signature purpose specifically to that user Ensures integrity of signed document to enable transportability of date, interoperability, verifiability and continuity of signature capability (verifying signature on document verifies the integrity of document and associated attributes and identity of signer)			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Electronic signature standard

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.310 (b)(2) Page 43269	Standard for electronic signature is digital signature	Electronic signature based upon cryptographic methods of originator authentication Computed by using set of rules and set of parameters so the identity of signer and integrity of data can be verified			
142.310 (c) Page 43269	If entity uses electronic signatures…	**Signature method must assure all of the following:**			
142.310 (c)(1) Page 43269	Message integrity	Assurance of unaltered transmission and receipt of message from sender to intended recipient			
142.310 (c)(2) Page 43269	Nonrepudiation	Strong and substantial evidence of identity of signer of a message and of message integrity, sufficient to prevent a party from successfully denying origin, submission or delivery of the message and the integrity of its contents			
142.310 (c)(3) Page 43269	User authentication	Provision of assurance of claimed identity of entity			
142.310 (d) Page 43269	Optional implementation features	**If entity uses electronic signatures, entity may also use, among others, any of following:**			
142.310 (d)(1) Page 43269	Ability to add attributes	One possible capability of digital signature technology (e.g., ability to add a time stamp as part of signature)			
142.310 (d)(2) Page 43269	Continuity of signature capability	Concept that public verification of signature must not compromise ability of signer to apply additional secure signatures at later date			

SECURITY REGULATIONS (PROPOSED RULE)

SECURITY STANDARD (CONTINUED)

Electronic signature standard

REGULATION/PG Part 142 Subpart C	SUBJECT Security Standard	ACTION	INTERPRETATIONS FROM PREAMBLE	IMPLEMENTATION	TOOLS TO IMPLEMENT
142.310 (d)(3) Page 43269	Countersignatures	Capability to prove order of application of signatures. Analogous to normal business practice of countersignatures, where party signs a document that has already been signed by another party			
142.310 (d)(4) Page 43269	Independent verifiability	Capability to verify signature without cooperation of signer			
142.310 (d)(5) Page 43269	Interoperability	Applications used on either side of communication, between trading partners and/or internal components of entity to enable the reading and correct interpretation of information communicated			
142.310 (d)(6) Page 43269	Multiple signatures	Multiple parties are able to sign document.			
142.310 (d)(7) Page 43269	Transportability of data	Ability of signed document to be transported over insecure network to another system while maintaining integrity of document, including content, signatures, signature attributes, and (if present) document attributes			
142.312 Page 43269	Effective dates				
142.312(a) Page 43269	General rules				
142.312(a)(1) Page 43269	Entities (except small health plans)	Must comply 24 months after effective date			
142.312(a)(2) Page 43269	**Delay ineffective date of standard transactions…**	**Does not delay implementation of security requirements**			
142.312(a)(3) Page 43269	Requirements…	May be implemented over time but must be completed by effective date			
142.312(b) Page 43269	Small health plans	Must comply 36 months after effective date			